

REMARKS

I. INTRODUCTION

Claims 1, 2, and 4 have been amended. Claim 3 has been cancelled. Support for the claim amendments can be found at least at page 4, lines 1-19 of the originally filed application. Thus, claims 1, 2, and 4 remain pending in this application. No new matter has been added. In view of the above amendments and the following remarks, Applicant respectfully submits that all presently pending claims are in condition for allowance.

II. THE 35 U.S.C. § 103(a) REJECTIONS SHOULD BE WITHDRAWN

Claims 1-4 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Herle et al. (U.S. Patent No. 7,013,391).

Claim 1, as amended, recites, “[a] method of distributing the location of a mobile device comprising the steps of: determining the location of the mobile device encrypting the determined location using an encryption key; transmitting the encrypted location to a server; storing the encrypted location at the server; querying the server from a remote terminal; transmitting from the server to the remote terminal the encrypted location in response to the query; *sharing the predetermined encryption key between the mobile device and the remote terminal by attaching the encryption key to a communication between the mobile device and the remote terminal, wherein the encryption key is not shared with the server*; and decrypting the location at the remote terminal using the predetermined encryption key.”

To meet the emphasized portion of claim 1 cited above, the Examiner relies on Herle’s disclosure of one embodiment in which “if the client access device properly authenticates, MS location server 160 transmits the encrypted MS 111 position data to the client access device, which then decrypts the MS 111 position data.” (See Examiner’s answer p. 4) (referring to Herle, col. 6, ll. 52-56). The Examiner states that in view of this portion of Herle’s disclosure, it would have been obvious to one of ordinary skill in the art would understand that Herle is suggesting that the encryption key is not given to

MS location server (160) but “only to those having authorization from the mobile station user.” (*Id.* at pp. 4-5).

Claim 1 has been amended to recite that the encryption key is shared with the remote terminal as an attachment to a communication between the mobile device and the remote terminal. Applicant respectfully submits that even if the Examiner can infer that the mobile station (111) shares the encryption key(s) (282) with the client access device and not the MS location server (160), there is no indication whatsoever how this would be done. Accordingly, Herle fails to disclose or suggest “sharing the predetermined encryption key between the mobile device and the remote terminal *by attaching the encryption key to a communication between the mobile device and the remote terminal*, wherein the encryption key is not shared with the server,” as recited in claim 1.

It is, therefore, respectfully submitted that claim 1 is allowable. Independent claims 2 and 4 recite limitations substantially similar to those of claim 1. Thus, Applicant respectfully submits that these claims are allowable for at least the foregoing reasons presented with regards to claim 1.

CONCLUSION

In view of the above remarks, it is respectfully submitted that all the presently pending claims are in condition for allowance. All issues raised by the Examiner having been addressed, an early and favorable action on the merits is earnestly solicited.

Respectfully submitted,

Dated: February 2, 2011

By: /Michael J. Marcin/
Michael Marcin (Reg. No. 48,198)

Fay Kaplun & Marcin, LLP
150 Broadway, Suite 702
New York, NY 10038
Phone: 212-619-6000
Fax: 212-619-0276